

International Conference on Biometrics and Ethics
Ronald Reagan Building
Washington, D.C.

November 28 – 29, 2006

Summary

The International Conference on Biometrics and Ethics, held November 28-29 in Washington, DC, brought together approximately 80 experts from several countries to engage in an open discussion of the application and ethics of biometrics. To achieve the objective of a candid exchange of ideas, the meeting was open to invitees only, with the exception of two keynote addresses by appointed officials. Co-hosted by the U.S. Department of Homeland Security (DHS) Privacy Office, US-VISIT and Biometrics Coordination Group, the conference was the second of its kind, following one that had been held in Brussels in 2005. Participants included representatives from academia, private industry, non-profit organizations, and government, hailing from Asia, Europe, the Middle East and North America. In addition to DHS, representatives from the U.S. Departments of Defense, Justice and State also attended.

The Conference featured keynote speeches by Mr. Stewart Baker, Assistant Secretary for Policy, DHS; Mr. Ben Riley, Director for Defense Biometrics, U.S. Department of Defense (DOD); Mr. Robert A. Mocny, Acting Director for the US-VISIT Program, DHS; and Dr. Emilio Mordini, Professor of Bioethics, University La Sapienza, Rome. Press covered Stewart Baker and Bob Mocny speeches. The four panel sessions featured presentations on: Privacy & Ethics under Normal and Extraordinary Circumstances; Ethics of Medical and Health Risks; Ethics of International Data Sharing; and Government-Industry Collaboration.

On Day 1, Stewart Baker's morning keynote addressed the use of biometrics in the US-VISIT program after Sept. 11. He warned against intentionally placing limitations on who has access to biometrics databases because this could inhibit vital information sharing.

In the session on Privacy & Ethics under Normal and Extraordinary Circumstances, participants discussed the definitions of the terms "extraordinary circumstances," "ethics" and "biometrics." Participants considered whether laws should be written to apply to extraordinary circumstances or be overridden in such cases. Conversation also ensued on whether existing privacy guidelines need to be modified for biometrics. One participant urged those involved with the creation and management of biometrics databases to "anticipate the unanticipated, because it will happen." Participants debated the value of consent, transparency and disclosure in the use of biometrics in identity management and security programs.

Ben Riley's lunch keynote focused on how the DOD employs biometrics and the Department's new structure to focus on biometrics technology and implications for privacy and other ethical issues.

In the session on the Ethics of Medical and Health Risks, discussion centered on fingerprint-scanner devices and the possibility of infectious diseases to be transmitted via these devices. Participants emphasized the effects of public perception on the success of biometric programs. Many participants argued that transparency, redress mechanisms and a right to anonymity must be

considered by policy-makers and systems designers in the modern era where biometrics such as fingerprints permanently memorialize identity.

On Day 2, Dr. Emilio Mordini's morning keynote focused on the importance of accepted criteria for the use of biometric technology to properly identify individuals, given the political relevance of accurately establishing identity.

The session on the Ethics of International Data Sharing covered examples of how biometric data is currently shared or can be shared between countries, and what countries are currently doing to protect privacy. Participants debated the assertion that the international community has widely divergent views about acceptable levels of data protection, and discussed ethical bases for data exchange. The concept of reciprocity was raised, along with the idea of agreement on common international privacy principles as a framework for the use of biometric data.

Bob Mocny's lunch keynote addressed the ethical imperative of governments to share information about criminals and those who would attempt to do harm. He described the U.S. government's vision of an infrastructure that provides a secure environment for information sharing that protects privacy.

The session on Government-Industry Collaboration examined the relationship between government and industry biometric applications. Examples illustrated how government and industry work together in symbiotic relationships, but also underlined the importance of having checks and balances to prevent the government and private industry from intentionally or unintentionally subverting privacy laws in these partnerships.

Several themes emerged from the two days of discussion: the critical need to study and develop guidance for use of biometrics, the need to apply fair information practices to biometrics and the potentially long-lasting implications of biometrics on societies and individuals. The presentations and discussions revealed the breadth of biometrics applications and their impact on society.

The conference set the groundwork for a third conference to further discuss the ethical issues of the use of biometrics for security purposes and identity management.